UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/653,503	09/02/2003	Len L. Mizrah	AIDT 1005-1	3753

22470 7590 11/07/2008

HAYNES BEFFEL & WOLFELD LLP
P O BOX 366
HALF MOON BAY, CA 94019

EXAMINER	
HOMAYOUNMEHR, FARID	

ART UNIT	PAPER NUMBER
2439	

MAIL DATE	DELIVERY MODE
11/07/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/653,503	MIZRAH, LEN L.	
	Examiner	Art Unit	
	Farid Homayounmehr	2439	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *28 July 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *2-4,6,7,9-11,13,14,16-18,20,21 and 31-39* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *2-4, 6, 7, 9-11, 13, 14, 16-18, 20, 21, and 31-39* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This action is responsive to communications: application, filed 9/30/2003; amendment filed 7/28/2008.

2. Claims 2-4, 6, 7, 9-11, 13, 14, 16-18, 20, 21, and 31-39 have been considered. Claims 1, 5, 8, 12, 15, 19, 22-30 cancelled by the applicant.

Response to Arguments

3. With regards to rejection under section 112, 1st paragraph, applicant argues that the computer readable mediums were part of original claims, and therefore are part of disclosure. This argument is found persuasive, and the rejection is hereby withdrawn.

Applicant objects to the Official Notice taken by the Examiner. Applicant states: "Applicant objects to the Official Notice stated at page 7, at the 6th and 5th lines from the bottom, reading "The nth and (n+1)th iterations also includes creating a hash of the session key, which the Examiner takes the Official Notice to be also a well-known technique in the art." Specifically, it is not clear what the "noticed fact" is intended to be." However, at the very beginning of the same paragraph, Examiner states: "*In other words, the above process is an iterative method, which involves application of a set of operations in each iteration, each of those operations identical to one of the operations*

discussed above." Therefore, it is clear that in said paragraph, Examiner is explaining the operations in each iteration, and how that operation is disclosed in the prior art. Therefore, it is clear that the subject of Official Notice in said phrase is that creating a hash of a session key is known in the art.

Applicant is also reminded that applicant can request an interview with the Examiner to clarify any ambiguity regarding the rejections or discuss the case. In fact, the best time for an interview is considered to be after the Non-Final rejection.

Applicant further argues that the session is not hashed and it is actually the intermediate keys that are hashed. However, Examiner's Official Notice shows that hashing a session key is known in the art, which also shows that hashing a key is known in the art. In addition, what the applicant calls an intermediate key has a similar role as a session key. Meaning both keys represent a key that is valid temporarily, evidence by the fact that both the session keys and intermediate keys are discarded after they are expired. Accordingly, applicant's argument regarding the subject of the Official Notice being unclear is found non persuasive.

Applicant requires documentary evidence that hashing a session key is known in the art. Applicant is required to provide seasonable argument detailing why the matter of notice is not well-known in the art. There is no such argument provided by the applicant, and Examiner is not required to provide such evidence. However, to reinforce the

Official Notice, Examiner points out US 2003/0185391 in paragraph [0055], which states:

[0055] At 331, client 301 sends a combined with other public information to server 303. The server 303 then performs a hash of the derived session key combined with the other information known to server 303 to verify the identity of the client 301. Similarly, at 335, server 303 sends a along with other information known to client 301 to allow client 301 to verify the identify of server 303. According to various embodiments, a cryptography accelerator with hash cores according to the techniques of the present invention makes generation of finished messages highly efficient.

This clearly shows hashing a session key for the purpose of verifying the identity of a party, which is exactly the subject matter of the claim.

Applicant also requires documentary evidence to support the Official Notice. However, to request documentary evidence to support an Official Notice, applicant must provide seasonable argument as to why the matter is not well-known in the art. Applicant has presented no argument that hashing a session was not well-known in the art.

Under section titled Basis of Request for Reconsideration, applicant argues that the Office Action has not set forth a rationale for using the combination of steps recited in the claim. However, the Office Action clearly states the motivation for combining

elements of prior art. For example, when discussing the iterative portion of the applicant's invention, the Office Action notes that repeating a process is known in the art, and adds that the repetitive process is shown in DES protocol, with the clear motivation to make it more difficult for an intruder to break the encryption or discover the keys. The Office action clearly states that applicant's invention is regarded as the combination of several known steps and repeating those steps in an iterative manner. The rejection states that the combination of steps and repeating the combination of steps would be obvious, unless it produces an unexpected result. It is up to the applicant to show an unexpected result that makes the invention non obvious over the combination of elements cited from the prior art. The following is the details of response to applicant's arguments:

At the top of page 7, applicant argues that Examiner has not interpreted the session initiation key interval correctly. Applicant argues: "The "session key initiation interval" in claim 31 is a time during which the particular session key will be used for initiation of a session." First, applicant does not specify any portion of the Specification in support of said definition. Second, the cited portion of Perlman shows that several session keys are available and they have an associated expiration date. The fact that the session keys have an expiration date does not necessarily mean that the lifetime of the key is the session initiation interval. Each session key is used for a session. Therefore, each key initiates a session for which it is used as the session key. Therefore, for each session key, there is an interval during which the particular session key is used for initiation of a

session. Clearly, the keys cannot be discarded before the session they initiated is expired. Therefore, the keys are discarded after the expiration of their session key initiation interval, which reads on the claim.

Applicant further argues: "In the process of claim 31, the "associated session key" is selected based on the session key initiation interval in which a request to initiate a communication session is received." However, this is a trivial interpretation. As discussed above, if the key's session key initiation interval is the time during which the particular session key will be used for initiation of a session, then the interval does not begin unless the key initiates a session. This also applies to Perlman system. Even if Perlman selects a key based on its expiration time, whenever a key is selected, a session initiation key interval begins when the key initiates a session. Therefore, it reads on the claim requirement.

Applicant further argues: "Specifically, and unlike the prior art, the associated session key is used to encrypt the digital identifier, and sent back to the first station, not to hide the digital identifier, but rather to verify receipt by the second station of the session key. The rationale set forth by the Examiner ignores this stated feature in the claim." However, Examiner's rationale does not ignore this feature. As mentioned by the applicant, Examiner's rejection mentions SSL. When standards such as SSL setup a session, they do rely on parameters sent from one party to other, to be returned by the other party for verification. Therefore, such feature is addressed in the associated rejection.

Applicant further argues: "With respect to this limitation, the Office Action states "this limitation creates n ephemeral keys, with the same characteristics of Perlman's ephemeral keys discussed above. An iterative process, which repeats the same steps, and how it is taught in the prior art is discussed in the following." Office Action, page 6. From this just quoted comment, Applicant surmises that the Examiner is reading the claim limitation "set of intermediate data keys" on keys other than the selected key in the table of Fig. 1 in Perlman." However, if the rejection states that the ephemeral keys have the same characteristics as Perlman's ephemeral keys, it is not clear why it is interpreted that the intermediate keys **other than** the keys in table 1 (Perlman's ephemeral keys). Therefore, applicant's interpretation is incorrect, and the argument is not persuasive.

Applicant further argues: "However, the Office Action does not establish the process of using an associated session key selected as required by the claim for this purpose." However, in addressing the claim limitation, the rejection does state that the limitations involve a repetition of a fundamental process. That fundamental process does include using associated session keys as indicated in the rejection. Therefore, the rejection does address the claim requirement.

Applicant further argues: "There is no process described in Perlman that involves sending one of the keys from the table in Fig. 1 encrypted using another of those keys." However, many

systems using ephemeral keys use the ephemeral key to establish another ephemeral key before the original ephemeral key is expired. The new ephemeral key is usually encrypted by the current ephemeral key and sent from one party to the other, before the current ephemeral key is expired. An example of such system is SSL, which is cited by Perlman. Also note that the concept of encrypting another key by the ephemeral is shown be Perlman col. 4 lines 28-37.

Applicant further argues: "The Examiner's comments on the claim limitations related to the "first set of exchanges" in claim 31 goes on to state "This whole process is discussed in the above." Applicant does not understand this comment, and requests clarification should the Examiner maintain this rejection on reconsideration." As mentioned in the Office Action in rejecting the limitations relative to the first set of exchanges: "In other words, the above process [limitations of the first set of exchanges] is an iterative method, which involves application of a set of operations in each iteration, each of those operations identical to one of the operations discussed above. Namely, during the first to the (n-1)th iteration, the system repeats sending a new key, encrypted from one station to the other. The new key is encrypted with a key known to both parties (the previous session key). The receiving side decrypts the encrypted new key and uses it as the new session key Column 5, lines 55 - Column 6, lines 20. Perlman's teaching of ephemeral keys is for the purpose substituting a key with another after the lifetime of a key is expired. Therefore, the session keys are substituted with a fresh key after expiration of their

lifetime. This whole process is discussed in the above." The last process above is actually the rejections associated with the first 5 paragraphs of claim 31.

Applicant again states that they don't understand what is meant by: This technique is also discussed above. Once again, the techniques refer to operations of the first 5 paragraphs of claim 31.

Applicant further states that the rejection provides no rationale as to why the operations of first and second exchanges would be obvious. However, the office action breaks down the claim limitations, shows that each element was known in the art, what the purpose of each element is, and why it is obvious to combine the elements. For instance, the rejection states that Perlman teaches establishing ephemeral keys for data exchange, Kelly teaches an authentication process which involves the same verification process as the one claimed, and performing those steps in iterative manner has the advantage of making it more difficult to discover the keys.

Applicant further argues that use of hash functions are known in the art, but the rejection does not show use of hash functions the same way as the claimed invention. However, the rejection includes citations from the book Applied Cryptography, which

uses the hash function for the same purpose, i.e. using it to verify the integrity of exchanged data, e.g. session or intermediate keys.

Applicant then agrees that iterative methods to improve the security of an encryption process, as exampled in DES are known in the art, but argues that there is no showing that the iterative method was used the same way as the claimed invention. However, the rejection outlines how the claimed invention, including iterative part would be obvious to the one skilled in art based on teachings of Perlman in view of Kelly, and the Official Notice.

Applicant further argues that the first set of exchanges does not have a shared secret, and only the second set of exchanges include a shared secret. However, Claim limitation reads:

"...the first set of exchanges including sending a message to the second station carrying intermediate data key (i) from said set of intermediate data keys encrypted using the associated session key for a first exchange in first set of exchanges and using the intermediate data key (i-1) for subsequent exchanges in the first set of exchanges," Therefore, the first set of exchanges includes sending data key (i) encrypted using the associated session key. In this instance, the session key, and in the subsequent exchanges, the intermediate data key (i-1) are considered the shared secrets. These shared secrets are updated from one iteration to the other, which is addressed by the

rejection. Therefore, the first set of exchanges does include a shared secret exchanged and established between the parties. Accordingly, there is no mischaracterization of the claimed invention in the associated rejections.

Applicant further argues that the first and second set of exchanges are not substantially the same. However, the associated rejection states that the second set of exchanges includes an iterative process, which makes it similar to the first set of exchanges in that the first set of exchanges also includes an iterative process. The differences between the first and second set of exchanges are mentioned in the rejection and addressed.

With regards to the last element of claim 31, applicant states that Kelly does not include ephemeral key encryption. However, ephemeral key encryption is taught by Perlman as addressed in details in rejection of claim 31.

Applicant further argues: "Furthermore, the Office Action has not set forth the rationale for using the combination of steps recited. Rather, it is based on the approach of addressing each of the steps taken alone.
Specifically, the elements set forth in the Office Action are chosen from the two references in the record that perform separate functions unrelated to the claimed invention, and vague Official Notice, and the chosen elements are pieced together in a manner only possible in light of the

present claims, and then a conclusion is presented without clear reasoning that the claims would have been obvious." However, the rejection includes a rationale and motivation for combining Perlman with Kelly. It also includes motivation to use well-known techniques of The Official Notice with Perlman in view of Kelly to teach the requirements of the claimed invention.

With regards to claim 32, applicant argues: "Turning to claim 32, the Office Action rejects this claim with the rationale "encryption using a key such as key (n-1) was well known in the art at the time of the invention. The motivation to do so would be to secure the message by delivering it in ciphertext rather than clear text." This rationale for rejection suggest that the mere fact that it is desirable to encrypt a message proves that it is obvious to do so in the specific manner claimed. The rejection is flawed because it does not address the specific limitation in the claim that requires the use of a specific intermediate data key, that had been used earlier for another specific purpose". However, It is well known in the art to use keys to encrypt messages. Therefore, the elements of claim limitation were known in the prior art, and there is stated motivation to combine the prior art teaching with the cited references to come up with the claimed invention, as required to establish a prima-facie case of obviousness. Also, the intermediate key had been used for the purpose of secure exchange of data or messages. Claim 32 uses the intermediate key for the exact same purpose.

Regarding claim 33, applicant argues: "In fact, Perlman and Kelly do not relate to the distribution of symmetrical encryption key. Neither reference even describes a technique for doing so." However, Perlman Col. 2 line 63 to col. 3 line 3 clearly suggests establishment of ephemeral symmetric keys between parties.

With regards to claim 2, applicant argues: "The Examiner overlooks the fact that the session key is associated with the particular session key initiation interval, and selected based on that association." However, The session key and its association with a session key initiation interval is part of claim 31, and discussed and addressed in the rejection of claim 1. Therefore, the requirement is not ignored.

Applicant further states that the claim requirement is unlike any other in the prior art, without discussing the associated rejection which makes the limitations obvious over prior art.

With regards to claim 3, applicant argues that the claim is allowable because it depends on claim 2. However, as discussed above, claim 2 is not allowable.

Applicant further argues: "The Examiner has not provided any explanation of how Perlman suggests using the any keys in a process like that recited in the present claims." However, rejection of claim 3 includes an explanation on how the claim requirements are made obvious over prior art. Applicant does not discuss the associated rejection.

Applicant further argues: "Furthermore, the keys described in Perlman are final encryption keys, not applied to any iterative process, as mentioned above in connection with the rejection of claim 31." However, application of encryption keys in an iterative process is discussed in rejection of claim 31.

With regards to claim 4, applicant argues: "Specifically, in the analysis of the session key initiation interval in claim 31, the Examiner read the "session key initiation interval" on the expiration time of the keys in Perlman. With respect to claim 4, the Examiner is taking a position that the initiation interval is different than the lifetime. Any coherent rejection of these claims cannot have it both ways." However, as mentioned in the discussion relative to claim 31, the Examiner does not read the "session key initiation interval" on the expiration time of the keys in Perlman. Therefore, there rejection does not need have it both ways.

Applicant further argues: "In fact, the concept of an initiation interval that is associated with a session key used as claimed herein, is not found in Perlman or any of the references in the

record." However, the rejection of claim 31, and the above discussion associated with rejection of claim 31 shows how said claim limitation is made obvious over prior art.

With regards to claim 6, applicant merely mentions that the claim is dependent on claim 4, and has additional claim requirements, without any discussion of the associated rejection.

With regards to claim 7, applicant argues that the claim should be allowable because of its dependency on claim 4. However, as discussed above, claim 4 is not allowable.

Applicant also argues: "This generic idea provides no teaching whatsoever of a limit on the lifetime of the key as recited in claim 7." However, the rejection of claim 7 includes citation from Perlman that shows that the lifetime of the ephemeral keys can be set arbitrarily. The rejection further discusses how the claim limitation is made obvious over teachings of Perlman and what is well-known and/or logical in the prior art.

Based on the discussion above, applicant's argument relative to allowability of the pending claims is found non persuasive. The associated rejections are as follows:

Specification

4. The disclosure is objected to because claims 37- and 39 are directed to "machine readable data storage medium". The Specification does not describe "machine readable data storage medium". See MPEP 608.01(o).

Appropriate correction is required.

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 2-4, 6, 7, 9-11, 13, 14, 16-18, 20, 21, and 31-39 are rejected under 35 U.S.C. 103(a) as being unpatentable over Perlman, (US patent 6363480, March 26, 2002), in view of Kelly (US Patent No. 5,636,280, dated June 3,1997), and further in view of Official Notice.

6.1 As per claim 31, Perlman is directed to a method for mutual authentication in communications between first and second stations, comprising:

generating and storing a set of ephemeral session keys at the first station, ephemeral session keys in the set being associated with respective session key initiation intervals, and being discarded at a time later than expiration of the respective session key initiation intervals (fig. 1 and the associated text, particularly col. 5 lines 10-25);

in response to a request to initiate a communication session received by the first station during a particular session key initiation interval, selecting the associated session key (col. 6 lines 1-20);

sending a message carrying said associated session key to the second station (col. 6 lines 17-20),

and receiving a response from the second station including a digital identifier, the digital identifier being information shared between the first station and the second station, or between the first station and a user at the second station, the digital identifier being encrypted using said associated session key to verify receipt of the session key by the second station and to identify the second station or the user of the second station (Perlman col. 6 lines 21- 35 teaches receiving a message from the second party, encrypted with the communicated session key (note that Perlman col. 2 lines 20-35 suggests using short term keys (ephemeral) in setting up a session key. The SSL protocol certifies and authenticates the keys established to secure the communication session). However, Perlman does not specifically teach a digital identifier, the digital

identifier being information shared between the first station and the second station, or between the first station and a user at the second station, the digital identifier being encrypted using said associated session key to verify receipt of the session key by the second station and to identify the second station or the user of the second station. Kelly teaches authentication of parties of communication to each other and verification of session key based on a shared secret. Kelly col. 7 lines 5-50 specifically teach after the session key is established, in item (d) of the authentication protocol, a password (shared secret) is encrypted using the session key and sent to the host. The host verifies the password, and authenticates the other party.

Perlman and Kelly are analogous art as they are both directed to key distribution and user authentication in security systems based on cryptographic processes.

At the time of invention, it would have been obvious to the person skilled in art to combine the method of secured key exchange as taught by Kelly with the method of ephemeral key distribution as taught by Perlman. Kelly teaches a method to securely deliver keys from one party to another. Perlman teaches use of multiple ephemeral keys to secure the communication session, which requires transmission of ephemeral keys from one party to the other. Therefore, the one skilled in art would be motivated to use the method of Kelly to deliver the ephemeral keys of Perlman from one party to the other.);

generating and storing, in the first station, a set of intermediate data keys, the set of intermediate data keys including intermediate data key (i), for i = 1 to at least n, and being discarded at a time later than expiration of the particular session key initiation interval (this limitation creates n ephemeral keys, with the same characteristics of Perlman's ephemeral keys discussed above. An iterative process, which repeats the same steps, and how it is taught in the prior art is discussed in the following);

executing a first set of exchanges including one or more exchanges with the second station, after verifying in said first station receipt of the session key by the second station by decrypting the digital identifier using the associated session key at the first station and positively matching the decrypted digital identifier against an existing entry in a stored list of authorized users (the verification of the digital identifier at the first party is discussed in Kelly col. 7 lines 5-50),

the first set of exchanges including sending a message to the second station carrying intermediate data key (i) from said set of intermediate data keys encrypted using the associated session key for a first exchange in first set of exchanges and using the intermediate data key (i-1) for subsequent exchanges in the first set of exchanges, receiving a response from the second station including a hashed version of intermediate data key (i) encrypted using intermediate data key (i), decrypting the hashed version of the intermediate data key (i), calculating a hashed version of intermediate data key (i) at

the first station, and matching the calculated hashed version and the received hashed version of intermediate data key (i) to verify receipt by the second station of intermediate data key (i) (this process repeats the steps discussed in the first exchange of messages, by using the key verified in the first iteration in the second iteration (key (i) and Key (i-1)).

In other words, the above process is an iterative method, which involves application of a set of operations in each iteration, each of those operations identical to one of the operations discussed above. Namely, during the first to the (n-1)th iteration, the system repeats sending a new key, encrypted from one station to the other. The new key is encrypted with a key known to both parties (the previous session key). The receiving side decrypts the encrypted new key and uses it as the new session key Column 5, lines 55 - Column 6, lines 20. Perlman's teaching of ephemeral keys is for the purpose substituting a key with another after the lifetime of a key is expired. Therefore, the session keys are substituted with a fresh key after expiration of their lifetime. This whole process is discussed in the above. In the nth and (n+1)th iteration, the same process continues, with the exception that in the nth iteration the shared secret is used to encrypt the new key, and in the (n+1)th iteration a second shared secret is use for the same. This technique is also discussed above. The nth and (n+1)th iterations also includes creating a hash of the session key, which the Examiner takes the Official Notice to be also a well-known technique in the art. Therefore, all steps of the iterative method are discussed, and shown as prior art in the above. Also, using an iterative

technique to improve the security of the cryptographic protocol is well known in the art. Reference is made to the DES protocol, which basically deploys a plurality of stages that scrambles the input data iteratively, and each iterative stage uses a different parameter (a key) to perform a different operation. The key in each stage is extracted from the previous stage. As another example, reference is made to "Applied Cryptography" by B. Schneier, page 53 (a copy is attached to this Office Action). Section titled SKEY, clearly teaches the concept of repeated application of a cryptographic technique to improve the security of the protocol. Therefore, given enough resources and time, it would have been obvious to use an iterative method, which includes a known process at each iterative stage to improve the security of the protocol.);

executing a second set of exchanges for mutual authentication after verifying in said first station receipt of the intermediate data key (n-1) by the second station, including sending a first message carrying intermediate data key (n) encrypted using a hashed version of a first shared secret,
receiving a response from the second station carrying a hashed version of intermediate data key (n) encrypted using a hashed version of the first shared secret, and decrypting the hashed version of the intermediate data key (n), calculating a hashed version of intermediate data key (n) at the first station, and matching the calculated hashed version and the decrypted hashed version of intermediate data key (n) to verify possession by the second station of the first shared secret;

sending a second message carrying intermediate data key (n) encrypted using a hashed version of a second shared secret; and

if the second station sends a response to the second message, carrying a hashed version of intermediate data key (n) encrypted using a hashed version of the second shared secret, after possession by the first station of the second shared secret is verified at the second station, the verifying being accomplished at the second station by decrypting the intermediate data key (n) from the second message using the hashed version of the second shared secret, calculating a hashed version of the intermediate data key (n), and matching the calculated hashed version and the decrypted hashed version of intermediate data key (n) to verify possession by the first station of the second shared secret, then receiving the response from the second station, and decrypting the hashed version of the intermediate data key (n) using the hashed version of the second shared secret, calculating a hashed version of intermediate data key (n) at the first station, and matching the calculated hashed version and the decrypted hashed version of intermediate data key (n) at the first station to verify mutual authentication of the first and second stations (the second set of exchanges again involves an iteration process, similar to what is discussed above, with a difference of using a second shared secret in addition to the first shared secret, and using a hashed version of an encryption key to encrypt the key. However, using the second shared secret is again repeating the same process where the first secret was used. Also use of a hashed version of a key is known in the art, as exemplified in DES protocol.);

and if mutual authentication is verified at the first station, then sending a message indicating successful authentication (Kelly Col. 6 lines 57-62).

6.2. As per claim 32, Perlman in view of Kelly, further in view of Official Notice is directed to the method of claim 31, wherein said message indicating successful authentication carries a signal encrypted using intermediate data key (n-1) or using another prearranged one of 3 said intermediate data keys (i) (encryption using a key such as key(n-1) was well known in the art at the time of invention. The motivation to do so would be to secure the message by delivering it in cipher text rather than clear text.

6.3. As per claim 33, Perlman in view of Kelly, further in view of Official Notice is directed to the method of claim 31, including using intermediate data key (n) as a symmetrical key to encrypt data during post-authentication communications between the first and second stations in the communication session (The purpose of establishing keys between parties of communication is encrypting the message for the purpose of confidentiality protection, or integrity protection).

6.4. As per claim 2, Perlman in view of Kelly, further in view of Official Notice is directed to the method of claim 31, including using said associated session key in response to another request to initiate a communication session from a third station received by the first station for first exchanges in the during said particular session key initiation interval, and using other session keys from the set of ephemeral session keys

after expiry of said particular session key initiation interval (Perlman in view of Kelly, further in view of Official Notice teaches use of a associated session key in response to a request to initiate a communication session from any station received by the first station for first exchanges in the during said particular session key initiation interval. Therefore, the combination teaches use of an associated session key in response to another request to initiate a communication session from a third station received by the first station for first exchanges in the during said particular session key initiation interval (see response to claim 31). The combination also teaches use of another set of ephemeral keys after one is expired).

6.5. As per claim 3, Perlman in view of Kelly, further in view of Official Notice is directed to the method of claim 3, including associating a unique set of intermediate data keys with each session key (the combination discloses the method of claim 2, including assigning said session random key to all communication sessions initiated with the first station during said session random key initiation interval, and associating a different set of ephemeral intermediate data random keys with each communication session, where the first party announces a set of ephemeral key pairs (Column 5, lines 55-67) and each time the second party desires to launch a communication session with the first party, a key is selected from the list (and therefore is unique), and the first party passes the key to the second party (Column 6, lines 1-20)).

6.6. As per claim 4, Perlman in view of Kelly, further in view of Official Notice is directed to the method of claim 31, including:
providing a buffer at the first station (Perlman Column 6, lines 35-57); storing the set of ephemeral session keys in the buffer (Column 5, lines 55- 67 & Column 6, lines 35-57. Note that the session keys are ephemeral keys and are stored only during their lifetime) and removing session keys from said buffer upon expiry of respective session key lifetimes, said session key lifetimes being longer than the respective session key initiation intervals (the ephemeral keys are removed from buffer when expired, as shown in claim 31. Per column 6, lines 35-67, the lifetime of Perlman's ephemeral keys is arbitrarily set to match the application. Setting the lifetime such that it is usable after the set up period is completed is a obvious, logical and trivial choice. It is a trivial choice to choose the lifetime of session keys to be longer than the initiation intervals because the initiation interval is part of the session).

6.7. As per claim 6, Perlman in view of Kelly, further in view of Official Notice is directed to the method of claim 4, wherein the session key lifetimes have respective lengths longer or equal to a time required for verification of mutual authentication using said first and second sets of exchanges for the plurality of exchanges used to distribute the symmetric in expected circumstances (Column 6, lines 35-67. The lifetime of Perlman's ephemeral keys is arbitrarily set to match the application. Setting the lifetime such that they last long enough for completion of verification is a logical and obvious choice).

6.8. As per claim 7, Perlman in view of Kelly, further in view of Official Notice is directed to the method of claim 4, wherein the session key lifetimes have respective lengths which are a multiple M times a time required for verification of mutual authentication using said first and second sets of exchanges in expected circumstances, where M is less than or equal to 10 (Column 6, lines 35-67. The lifetime of Perlman's ephemeral keys is arbitrarily set to match the application. Setting the lifetime such that the key is usable after any multiple of times it takes to complete the set up period is a logical and obvious choice).

6.9. Requirements of claims 9-11, 13-18, 20 and 21 are substantially the same as claims 31-33, 3, 4, 5-7 discussed above.

6.10. Requirements of claims 34-36, and 37-39 are substantially the same as claims 31-33 discussed above.

Conclusion

7. **THIS ACTION IS MADE FINAL**. See MPEP § 7.39. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within

TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

8. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Farid Homayounmehr whose telephone number is (571) 272-3739. The examiner can be normally reached on 9 hrs Mon-Fri, off Monday biweekly.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on (571) 272-3811. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Farid Homayounmehr

10/25/2008

/Kambiz Zand/

Supervisory Patent Examiner, Art Unit 2434